Catholic University Journal of Law and Technology

Volume 28
Issue 2 *Spring 2020*

Article 5

2020

# Protecting Online Privacy in the Digital Age: *Carpenter v. United States* and the Fourth Amendment's Third-Party Doctrine

Cristina Del Rosso
*University of Central Florida*

Carol M. Bast
*University of Central Florida*

# PROTECTING ONLINE PRIVACY IN THE DIGITAL AGE: *CARPENTER V. UNITED STATES* AND THE FOURTH AMENDMENT'S THIRD-PARTY DOCTRINE

*Cristina Del Rosso*[*] *& Carol M. Bast*[**]



[*] Cristina Del Rosso graduated with a Legal Studies major, specializations in Public Law and Law and Society, and a minor in Political Science on the prelaw track from the University of Central Florida, Orlando, Florida in Spring 2020. The foundation of this manuscript is the Honors in the Major thesis Cristina researched, wrote, and successfully defended in front of a committee of three professors. While at UCF, Cristina was heavily involved in the UCF Moot Court Team.

[**] Carol M. Bast is a professor in the Department of Legal Studies at the University of Central Florida, where she has taught for the past twenty-nine years. She teaches Legal Research and Legal Writing and authored an undergraduate textbook on those topics. She teaches the survey course, Law and the Legal System, and co-authored an undergraduate textbook used in the course. Her areas of research and writing include eavesdropping and wiretapping, plagiarism, legal ethics, legal research, legal writing, and international trade agreements. She served as Editor-in-Chief of the *Journal of Legal Studies in Business*, November 2008–November 2010; she served as Editor-in-Chief of the *Journal of Legal Studies Education*, August 2006–August 2008. Prior to becoming a professor, Bast clerked for a federal district judge and practiced corporate, securities, and real estate law. She received her LL.M. in International Economic Law and Policy from the University of Barcelona in 2016, her J.D., *magna cum laude*, from New York Law School in 1982, and her B.A. from Kalamazoo College in 1974.

The world has evolved. Modern society is largely dependent on technology, and there is a never-ending appetite for scientific development; there is often new technology released that is making lives more convenient, and more connected, than ever. Many Americans live in a world where every click and internet search leaves a digital trail which can be stored and stitched together to reveal an individual's innermost private life.[1] Current law provides minimal privacy protection to individuals, undermining Americans' Fourth Amendment safeguard that many hold essential to certain individual freedoms.[2] The Fourth Amendment to the United States Constitution states that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause."[3]

The terms "unreasonable" and "reasonable" have become basic principles that have been used to guide authority.[4] However, in today's increasingly digitally connected world, where one has little choice but to use the internet to function,

---

1 Daniel Zwerdling, *Your Digital Trail, and How It Can Be Used Against You*, NPR (Sept. 20, 2013), https://www.npr.org/sections/alltechconsidered/2013/09/30/226835934/your-digital-trail-and-how-it-can-be-used-against-you.

2 Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, BRENNAN CTR. FOR JUST. (June 29, 2015), https://www.brennancenter.org/our-work/research-reports/rethinking-privacy-fourth-amendment-papers-and-third-party-doctrine.

3 U.S. CONST. amend. IV.

4 Jonathan Kim, *Fourth Amendment*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/fourth_amendment (last updated June 2017).

there is a concern as to what exactly is "reasonable." This is because many smart devices share users' information with third parties.[5] In fact, in a world where digital technology has revolutionized the way in which Americans conduct daily business, many feel as if an expectation of privacy no longer exists.[6]

This sharing of information has led to a growing privacy gap that denies Fourth Amendment protection, more specifically the "third-party doctrine." In a briefing to members of Congress, the Congressional Research Service described the third-party doctrine as follows:

> In these cases, the Court held that people are not entitled to an expectation of privacy in information they voluntarily provide to third parties. This legal proposition, known as the third-party doctrine, permits the government access to, as a matter of Fourth Amendment law, a vast amount of information about individuals, such as the websites they visit; who they have emailed; the phone numbers they dial; and their utility, banking, and education records, just to name a few.[7]

In the increasingly digital world, companies hold a plethora of information on behalf of their customers, which these customers have voluntarily provided.[8] Information that is voluntarily provided is not protected by the Fourth Amendment; the Supreme Court has held that the information "a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[9] The doctrine has allowed the government to access information using a standard lower than probable cause.[10] This doctrine should be reassessed to better fit into the digital age. Property law, a reasonable expectation of privacy, and the trespass doctrine, to name a few standards of deciding what is private, are not promising steppingstones on which to continue to base Fourth Amendment claims.

Technological advancements and the proliferation of third-party records since

---

5 Lisa A. Schmidt, *Social Networking and the Fourth Amendment: Location Tracking on Facebook, Twitter and Foursquare*, 22 CORNELL J. L. & PUB. POL'Y 515, 524 (2012).

6 *See Scenario ONE: The New Normal*, U.C. BERKELEY CTR. FOR LONG-TERM CYBERSECURITY, https://cltc.berkeley.edu/scenario/scenario-one/ (last visited Apr. 20, 2020) (suggesting that by 2020, most of people's information will be kept online, leaving people vulnerable to data breaches, government intervention, and public display of sensitive information).

7 RICHARD M. THOMPSON II, CONG. RESEARCH SERV., R43586, THE FOURTH AMENDMENT & THIRD-PARTY DOCTRINE (2014).

8 Timothy Morey et al., *Customer Data: Designing for Transparency and Trust*, HARV. BUS. REV., May 2015, at 1, 4.

9 Katz v. United States, 389 U.S. 347, 351 (1967).

10 Margaret E. Twomey, *Voluntary Disclosure of Information as a Proposed Standard for the Fourth Amendment's Third-Party Doctrine*, 21 MICH. TELECOMM. & TECH. L. REV. 401, 410 (2015).

the doctrine's inception in two Supreme Court decisions in the late 1970s[11] raise questions about the stability of this doctrine in modern society.

The way the Supreme Court has historically looked at the Fourth Amendment is analogous to a patchwork quilt; the Supreme Court attempts to fix privacy concerns by evaluating technological advances one-by-one rather than considering what will come next or how one decision could impact future technologies. *Katz*,[12] *United States v. Jones*,[13] and *Riley v. California*[14] are Supreme Court cases that exhibit this piecemeal approach.

As technology transforms the way people participate in society, the core Fourth Amendment protection to feel secure in one's person, home, papers, and effects is beginning to erode. Under the third-party doctrine, the government can obtain any information that a person has disclosed to a third party, as the doctrine states that police do not need a warrant to search and seize consumers' private data on the internet.[15] Instead, the government or its agents can issue a subpoena to a third party, which is a non-governmental institution, in order to capture desired information.[16] As a result, the third-party doctrine allows the government to circumvent Americans' Constitutional guarantees without a warrant.[17] Under the third-party doctrine, the Fourth Amendment does not guarantee the privacy of personal data held by private companies, should the government request this information.[18]

In this way, the third-party doctrine acts as a general warrant as it is a blanket request that provides the government access to vast amounts of information retained by third-party service providers. General warrants were antithetical to the Founders' wishes at the founding of the country, and these wishes should be carried through in the interpretation of privacy rights today.[19]

*Carpenter v. United States* is the most recent Supreme Court case that takes issue with the third-party doctrine, specifically focusing on the relatively new

---

11 United States v. Miller, 425 U.S. 435 (1976); Smith v. Maryland, 442 U.S. 735 (1979).

12 *Katz*, 389 U.S. 347.

13 United States v. Jones, 565 U.S. 400 (2012).

14 Riley v. California, 573 U.S. 373 (2014).

15 Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 811 (2005).

16 *Id.* at 805.

17 Cristina Del Rosso, Protecting Online Privacy in the Digital Age: *Carpenter v. United States* and the Fourth Amendment's Third-Party Doctrine 3 (2019) (B.A. thesis, University of Central Florida) (on file with the University of Central Florida libraries).

18 Slobogin, *supra* note 15, at 811.

19 *See generally* Lee Arbetman & Michelle Perry, *Search and Seizure: The Meaning of the Fourth Amendment Today*, SOCIALSTUDIES, http://www.socialstudies.org/sites/default/files/publications/se/6105/610507.html (last visited Apr. 20, 2020) (discussing the history of the Fourth Amendment and how it applies to society today).

issue of how to treat cell-site location information ("CSLI").[20] In writing for the majority, Chief Justice Roberts opined that *Carpenter* was a narrow ruling that left existing precedent undisturbed and would not require law enforcement, in most cases, to obtain a warrant when seeking information held by third-party companies.[21] However, because the ruling was limited in only applying to CSLI, the parameters of this new-found protection remain unclear.

Society must reevaluate the third-party doctrine and the way it impacts lives both now and in the future, especially as it relates to emerging technology. This article proceeds in four sections. The first section reviews the Supreme Court's Fourth Amendment jurisprudence focused on the third-party doctrine and twenty-first century technology in order to examine how the current path for privacy rights is destined to fail. The second section examines how the current understanding of the doctrine applies to certain digital information like the information in *Carpenter*. The third section considers specific types of technology that store consumers' data and how the privacy they voluntarily share can be used against them in this digital age, particularly, how digital technologies threaten to exclude immeasurable quantities of personal information from Fourth Amendment protection. The final section offers a review of current theories of privacy and suggestions on how to proceed.

## I. THE LANGUAGE AND HISTORY OF THE FOURTH AMENDMENT

To discuss the inconsistencies of the Supreme Court's interpretation of the Fourth Amendment, a review of its origins and history is imperative. The first clause of the Fourth Amendment prohibits unreasonable searches and seizures, while the second clause specifically bans the use of "general warrants."[22]

The Warrant Clause, which is understood to be the second clause of the text, is thought to regulate warrant authority.[23] This clause is believed to ban the use of "general warrants," which are blanket warrants that can be obtained without an "adequate showing of cause."[24] They "allowed officers to search wherever they wanted and to seize whatever they wanted, with few exceptions."[25]

The Founding Fathers "sought to prevent unjustified searches" from occurring in the first place;[26] regardless of location, the Founders desired

---

20 Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).
21 *Id.* at 2220.
22 Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 551 (1999).
23 *Id.* at 558.
24 *Id.*
25 LEONARD W. LEVY, ORIGINS OF THE BILL OF RIGHTS 153 (1999).
26 *Id.* at 576.

protections for personal items.[27] Moreover, unlike the real property discussed in the text of the Amendment, effects could be carted away by the government.[28] The Founders did not seek a post-intrusion remedy; instead they implemented a deterrent to the government issuance of a nonspecific warrant.[29] Should an officer seize an item without a valid warrant, the citizen whose person, house, papers, or effects had been the subject of a trespass could hold the officer liable in tort.[30]

The Founders' goal in eliminating general warrants was to ensure that the oppressive practices of the crown in Great Britain could not be used in their new nation.[31] Famous English cases involving the search and seizure of papers to silence critics of the king struck a nerve with many of the colonies.[32] The first of these cases surrounds Mr. John Wilkes, who was accused of writing articles mocking the king and his ministers.[33] Wilkes was subjected to an invasive search under a general warrant and subsequently arrested.[34] Wilkes sought to enforce his right to security in his house and brought trespass actions against the officers who searched his property; the jury ultimately ruled in favor of Wilkes.[35]

The second case, which arose out of similar circumstances to *Wilkes*, was *Entick v. Carrington*,[36] a cornerstone case that "foreshadowed the requirements of the fourth amendment's search and seizure clause by holding that seizures of certain papers are impermissibly intrusive."[37] In *Entick*, the Secretary of State authorized a warrant to search for some documents on Entick's land.[38] In executing the warrant, many of Entick's books, papers, and pamphlets were seized.[39] Entick sued for trespass, leading the court to condemn the search and

---

27 Maureen E. Brady, *The Lost "Effects" of the Fourth Amendment: Giving Personal Property Due Protection*, 125 YALE L.J. 946, 985 (2016) ("[D]ictionaries from the period indicate that 'effects' was synonymous with personal property. . . .").

28 *Id.* at 991.

29 LEVY, *supra* note 25, at 577.

30 Akhil Reed Amar, *The Fourth Amendment, Boston, and the Writs of Assistance*, 30 SUFFOLK U. L. REV. 53, 60 (1996).

31 *Id.* at 74.

32 Eric Schnapper, *Unreasonable Searches and Seizures of Papers*, 71 VA. L. REV. 869, 887, 928 (1985).

33 *Id.* at 887, 887 n.102; Wilkes v. Wood (1763) 98 Eng. Rep. 489.

34 Schnapper, *supra* note 32, at 886–87 (explaining that the warrant failed to name Wilkes, and it did not specify items to be seized or particular places to be searched).

35 *Id.* at 887–88.

36 Entick v. Carrington (1765) 95 Eng. Rep. 807, 19 How. St. Tr. 1029. For a complete account on the *Entick* decision, look to the Howell's State Trials. They present "the Judgment itself at length, as delivered by the Lord Chief Justice of the Common-Pleas from written notes."; Schnapper, *supra* note 32, at 880.

37 Schnapper, *supra* note 32, at 876–77.

38 *Entick*, 19 How. St. Tr. at 1030–32; Schnapper, *supra* note 32, at 880.

39 *Entick*, 19 How. St. Tr. at 1030–32; Schnapper, *supra* note 32, at 880.

seizure; the court then held that the government could not seize private papers even with a valid warrant.[40] For the court, the issue was much deeper than the physical trespass; rather, it was concerned with protecting "the indefeasible rights of personal security, liberty, and private property."[41]

*Wilkes* and *Entick* served as an impetus to the Founding Fathers to ensure the types of governmental overreach that had occurred at the hands of the British were not adopted in their new nation. Instead, the Framers believed judicial officers were more adept at determining whether a search was reasonable,[42] favoring judicial approval for specific warrants to determine whether there were adequate grounds for intrusion.[43]

Although the Constitution does not expressly grant a right to privacy,[44] Fourth Amendment jurisprudence encompasses an expectation of privacy. In 1890, Samuel D. Warren and Louis D. Brandeis wrote about the legal right to privacy, declaring the right to privacy as an individual's "right of determining ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others."[45] Furthermore, they articulated privacy as the "right to be let alone."[46]

## II. THE THIRD-PARTY DOCTRINE AS A GENERAL WARRANT

The Framers loathed general warrants primarily because they did not want one individual with arbitrary discretion to decide when someone or something would be searched, especially with respect to "persons, houses, papers, and effects."[47]

*Wilkes* and *Entick* exemplify a time when the English government used general warrants to invade the privacy of its people at its own will.[48] This behavior is similar to the third-party doctrine, because the doctrine allows for the exercise of broad discretion when dealing with an individual and his or her effects.[49] Currently, the third-party doctrine enables the police and government

---

40 *Entick*, 19 How. St. Tr. at 1030–32; Schnapper, *supra* note 32, at 881.

41 Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1198 (2016).

42 Davies, *supra* note 22, at 577.

43 DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADE OFF BETWEEN PRIVACY AND SECURITY 4 (2011).

44 *See* Katz v. United States, 389 U.S. 347, 350 (1967) ("[T]he Fourth Amendment cannot be translated into a general constitutional 'right to privacy.' ").

45 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 198 (1890).

46 *Id.* at 193.

47 U.S. CONST. amend. IV.

48 *See* WILLIAM J. CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING 56–58, 96–100, 439–40, 490–91 (2009).

49 John Villasenor, *What You Need to Know About the Third-Party Doctrine*, THE ATLANTIC (Dec. 30, 2013), https://www.theatlantic.com/technology/archive/2013/12/what-

to engage in surveillance and monitoring of one's daily life, similar to the general warrant that the Fourth Amendment ultimately intended to prevent.[50] The Founding Fathers would have despised this doctrine.

In today's digitally connected world, the police only need to issue a subpoena to a third party to request desired data; there is no warrant requirement.[51] Without a specific warrant, the government is conducting the very type of general searches the Fourth Amendment was created to prevent.[52] This amendment guarantees citizens freedom from arbitrary government intrusion.[53] It rests on the right to be free from government surveillance unless there is probable cause.[54]

The third-party doctrine ignores the warrant requirement in the Fourth Amendment and allows the police to circumvent a warrant request from a judge, undermining free society and creating a culture of routine surveillance.

## III. THIRD-PARTY DOCTRINE CASE REVIEW

The progression of case law can help determine whether the third-party doctrine should still govern access to information as technology becomes increasingly complex and common. The following Supreme Court cases detail the development of the third-party doctrine.

*Katz* is the starting point for many Fourth Amendment cases because this is where the Supreme Court established the reasonable expectation of privacy test, which was articulated in Justice Harlan's concurrence.[55] Harlan's two-part framework first asks whether an individual retained an "actual (subjective) expectation of privacy," and second, whether that expectation is one that "society is prepared to recognize as 'reasonable.' "[56] The party must satisfy both prongs of this test to claim there has been an intrusion that is recognized under the Fourth Amendment.[57] The court has since endorsed this framework and considers it to be controlling in Fourth Amendment analysis.[58]

---

you-need-to-know-about-the-third-party-doctrine/282721/.

50 *Id*.

51 *See* Slobogin, *supra* note 15, at 826.

52 *Id*.

53 Katz v. United States, 389 U.S. 347, 353 (1967).

54 *Id.* at 356–57.

55 *See id.* at 360–62 (Harlan, J., concurring).

56 *Id*. at 361 (Harlan, J., concurring).

57 *Id*.

58 Mike Godwin, *What's Next for the Reasonable Expectation of Privacy? The Supreme Court's Ruling in* Carpenter *Raises New Questions.*, SLATE (June 27, 2018), https://slate.com/technology/2018/06/after-the-supreme-courts-carpenter-ruling-where-is-the-reasonable-expectation-of-privacy-heading.html.

In *Katz*, the court held that electronically listening to and recording the defendant's words by wiretapping a public phone booth, the door of which was closed, violated the defendant's privacy.[59] Because the defendant in *Katz* took a reasonable step to protect his privacy by shutting the door to the booth,[60] he was likely more concerned about an "uninvited ear" than an "intruding eye."[61]

Prior to *Katz*, the court had held that searches typically had to occur in someone's home; however, after *Katz*, a physical intrusion was no longer necessary to constitute a search under the Fourth Amendment.[62] In establishing these new provisions, the court reasoned that "the Fourth Amendment protects people, not places. . . . [W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[63]

*Miller* and *Smith* are two of the most significant Fourth Amendment cases decided by the Supreme Court in the twentieth century.[64] These cases preceded the rise of mass digital information aggregation, and, since these cases, there has been a surge of data collection and processing.[65] In *Miller*, the respondent was suspected of running an illegal whiskey distillery.[66] Federal agents subpoenaed his bank records and Miller objected, claiming his bank records were his private papers.[67] The court overruled this objection, holding that because the banking information was shared voluntarily with the banks, Miller forfeited his privacy attached to his financial records.[68] Since the information was voluntarily shared, Miller had not been searched under *Katz*.[69] In reaching this conclusion, the court distinguished "confidential communications" from "negotiable instruments to be used in commercial transactions," finding that bank records fit into the latter category.[70] *Miller* suggests that when documents are voluntarily conveyed to a third party, regardless of the purpose of conveyance, the individual relinquishes an expectation of privacy in those documents.[71]

A few years later, the Supreme Court decided *Smith*, holding that a warrant is not required when a telephone company voluntarily agrees to record a particular

---

59 *Katz*, 389 U.S. at 353.
60 *Id.* at 352.
61 *Id.*
62 *Id.* at 353; Olmstead v. United States, 277 U.S. 438, 464, 466 (1928) *overruled by* Katz v. United States, 389 U.S. 347 (1967).
63 *Katz*, 389 U.S. at 351.
64 THOMPSON II, *supra* note 7, at 9.
65 *Id.* at 2, 23–25.
66 United States v. Miller, 425 U.S. 435, 436 (1976).
67 *Id.* at 436, 438–39.
68 *Id.* at 437, 442–43.
69 *Id.* at 443.
70 *Id.* at 442.
71 *Id.* at 443.

user's telephone number records and to furnish said records to the police.[72] The court noted that because most people at the time were aware that the phone company recorded the phone numbers they dialed by using pen registers, there was no legitimate expectation of privacy.[73] In addition, because the information was voluntarily disclosed, Smith assumed the risk that the telephone company might disclose the information to the police.[74] The court further reasoned:

> The switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber. Petitioner concedes that if he had placed his calls through an operator, he could claim no legitimate expectation of privacy. We are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate.[75]

In *Smith*, the presence of technology did not alter the application of the third-party doctrine.[76]

The court differentiated *Smith* from *Katz*, stating that the pen registers at issue in *Smith* "[did] not acquire the contents of communications," as in *Katz*.[77] Justice Stewart further clarified the line between content and non-content general records in his *Smith* dissent:

> Nevertheless, the Court today says [Fourth Amendment] safeguards do not extend to the numbers dialed from a private telephone, apparently because when a caller dials a number the digits may be recorded by the telephone company for billing purposes. . . . The telephone conversation itself must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment. Yet we have squarely held that the user of even a public telephone is entitled "to assume that the words he utters into the mouthpiece will not be broadcast to the world."[78]

In dissent, Justice Stewart explained that people retain a reasonable expectation

---

72 Smith v. Maryland, 442 U.S. 735, 745–46 (1979).

73 *Id.* at 743; *Pen Register*, BLACK'S LAW DICTIONARY (11th ed. 2019) (defining a pen register as "an electronic device that tracks and records all the numbers dialed from a particular telephone line, as well as all the routing, addressing, or signaling information transmitted by other means of electronic communications").

74 *Smith*, 442 U.S. at 744.

75 *Id.* at 744–45 (citations omitted).

76 *Id.* at 742–45.

77 *Id.* at 741.

78 *Id.* at 746–47 (Stewart, J., dissenting) (quoting Katz v. United States, 389 U.S. 347, 352 (1967)).

of privacy in their conversations regardless of where they occur.[79]

In 2012, the court decided *United States v. Jones*.[80] In *Jones*, government agents installed a Global Positioning System ("GPS") tracking device on the defendant's vehicle without a valid warrant.[81] Ultimately, the placement of the device constituted a "search" within the meaning of the Fourth Amendment; the majority returned to pre-*Katz* doctrine, emphasizing the fact that because the government had physically attached the GPS device to the vehicle (an effect), the government had physically intruded, and therefore, a search had occurred.[82]

A year later, the court examined the warrantless search and seizure of cellular telephone contents incident to arrest in *Riley v. California*.[83] The Supreme Court created yet another exception to the Fourth Amendment when it decided that a warrant must be obtained from a judicial officer before law enforcement officers can search the contents of a phone.[84] Although the third-party doctrine was not discussed at length in *Riley*, the opinion did demonstrate the court's recognition of the difficulties that consumers and courts face when assessing whether an individual has a reasonable expectation of privacy in information stored on electronic devices.[85] The importance of *Riley* becomes clear when considering if the data the government is interested in resides on the device because, if so, then it should receive the same Fourth Amendment protections as data stored on a computer or a cellphone.[86] The court in *Riley* also considered the immense storage capacity that is available on cellphones; modern cellphones gather information and store that information in one place, thus the records can provide a detailed look into an individual's life.[87]

Thus, *Jones* is controlling with respect to GPS searches with a physical trespass, and *Riley* is controlling when searching a cellphone's data. *Jones* and *Riley* were the Supreme Court's first steps in addressing technology in the digital age. The *Carpenter* case is a blend of these two cases; the case involves long term tracking like in *Jones*, as well as a device that can pinpoint location with near-perfect accuracy, like in *Riley*.

In *Carpenter*, the petitioner was charged with aiding and abetting robbery that affected interstate commerce after the FBI obtained orders from a magistrate judge for cellphone records[88] under the Stored Communications Act ("SCA").[89]

---

79 *See id.* at 747 (Stewart, J., dissenting).
80 United States v. Jones, 565 U.S. 400, 404 (2012).
81 *Id.* at 403.
82 *Id.* at 404.
83 Riley v. United States, 573 U.S. 373, 378–79 (2014).
84 *Id.* at 401.
85 *Id.* at 385.
86 *Id.* at 397.
87 *Id.* at 392–395.
88 Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).
89 Stored Communications Act, 18 U.S.C. §§ 2701–2711 (2012).

This act, enacted by Congress as Title II of the Electronic Communications Privacy Act ("ECPA"), set forth provisions detailing privacy expectations with respect to means of electronic transmission, which include telephones and computers.[90] With *Carpenter*, the act gave the government access to petitioner's CSLI obtained from a third-party cellphone service provider that would otherwise be private information.[91] CSLI is produced when a phone user sends or receives data, such as phone calls or text messages, which are then transmitted to the closest cellular tower through radio waves, thus producing precise records.[92] These records include the date and time of transmitted data and the approximate location of where the call began and ended based on the proximity of the nearest cell tower.[93] Under the SCA, law enforcement does not need to obtain a search warrant in order to access these records; rather, law enforcement must only obtain a court order by meeting the reasonable suspicion standard, which is below the probable cause standard that must be met in order to secure a warrant.[94]

In *Carpenter*, the police obtained a court order permitting a search of Carpenter's cell records, pursuant to the Stored Communications Act.[95] To receive this order, law enforcement demonstrated their strong belief to the government that the records would be relevant to a robbery investigation after receiving tips from one suspect who provided the accomplice's cellphone number.[96] The government collected "12,898 location points cataloging Carpenter's movements," which is "an average of 101 data points per day"[97] over 127 days.[98] Using these location points, Carpenter was placed at the scene of four robberies in question, leading to Carpenter's conviction and a prison sentence of one-hundred years.[99] Following the conviction and appeal, the Supreme Court granted certiorari.[100]

---

90 *Id*. § 2702(a)(2)(A).
91 *Carpenter*, 138 S. Ct. at 2226.
92 Alexander Monteith, *Cell Site Location Information: A Catalyst for Change in Fourth Amendment Jurisprudence*, 27 KAN. J.L. & PUB. POL'Y 82, 84 (2017); *see How to Track Your Cell Phone*, WHIZ CELLS (Sept. 27, 2018), https://www.thewhizcells.com/how-to-track-your-cell-phone/.
93 *Carpenter*, 138 S. Ct. at 2225 (Kennedy, J., dissenting).
94 18 U.S.C. § 2703(d); Monteith, *supra* note 92, at 82–83.
95 *Carpenter*, 138 S. Ct. at 2212.
96 *Id*.
97 *Id*. at 2209.
98 *Id*.
99 *Id*. at 2212–13.
100 *Id*. at 2213.

A. The New Rule of *Carpenter*

Prior third-party doctrine cases, like *Miller* and *Smith*, left individuals with no legitimate Fourth Amendment expectation of privacy claim in information voluntarily shared with third parties.[101] At first blush, because CSLI is held by carriers (i.e. third parties) and not customers, *Carpenter* appeared to fall under this doctrine, leaving U.S. citizens vulnerable to retrospective location-tracking and warrantless searches on behalf of the government.[102] In writing for the majority, Chief Justice Roberts took a different approach.

Roberts wrote, "As technology has enhanced the Government's capacity to encroach upon areas normally guarded against inquisitive eyes, this Court sought to 'assure [] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.' "[103] He added that because "an individual maintains a legitimate expectation of privacy in the record of his physical movements," the third-party doctrine does not extend to mobile location information.[104]

Because CSLI is no more than a byproduct of owning a cellphone, the government generally needs a warrant to access those records, especially if the government is requesting more than seven days of records from the cellphone carrier.[105] According to the majority in *Carpenter*, the police cannot collect historical CSLI from a cellphone service provider due to its "depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection."[106] If the depth and reach of the surveillance threatens to become "a too permeating police surveillance," it may be justifiable to designate the search as an intrusive search under the Fourth Amendment.[107]

Due to the "world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today,"[108] the majority declined to extend the third-party doctrine to the government's request for CSLI.[109] Although the court noted that "seismic shifts in digital technology" have transformed the traditional third-party doctrine, Chief Justice Roberts

---

101 Smith v. Maryland, 442 U.S. 735, 743–44 (1979); United States v. Miller, 425 U.S. 435, 442 (1976).

102 *Carpenter*, 138 S. Ct. at 2217.

103 *Id.* at 2214 (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)).

104 *Id.* at 2217.

105 *Id.* at 2212, 2217. The Court did not explain why seven days is the maximum for surveillance. Subsequent cases will have to weigh this cutoff against privacy interests. *Id.*

106 *Id.* at 2223.

107 *Id.* at 2214 (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

108 *Id.* at 2219.

109 *Id.* at 2220 (finding that CSLI "implicate[d] privacy concerns far beyond those considered in *Smith* and *Miller*").

limited the language of *Carpenter* beyond the application of *Smith* and *Miller*, stating the decision does not "call into question conventional, surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information."[110]

Rather than close this gap in legislation, the court in *Carpenter* crafted a narrow exception to the third-party doctrine for the "unique nature of cell phone location records," requiring the government to obtain a warrant "[b]efore compelling a wireless carrier to turn over a subscriber's CSLI."[111] The court made sure to emphasize that this ruling did not impact *Miller* and *Smith*.[112]

This effort to limit the scope of *Carpenter* raises questions about the vast amount of information that resides outside of the outdated pen registers discussed in *Smith* and the paper bank statements at issue in *Miller*; nowadays, "the Government can access each carrier's deep repository of historical location information" with "just the click of a button."[113] The court also clarified that there is no distinction between the contents of cellphones and the CSLI metadata they generate.[114] The availability of all this information causes concern when one considers how common technology is in society and the vast amount of information that is shared online.

*Carpenter* raises questions about the continued validity of the *Katz* test in a digital world.[115] Evolving technologies transform which expectations of privacy are considered "reasonable," as Justices Thomas and Gorsuch have noted.[116] At the time *Miller* and *Smith* were decided, forfeiting privacy rights on a tangible item like a pen register or a bank document seemed reasonable.[117] However, applying the third-party doctrine to online activity, where most of the data is stored in one place, poses challenges. As Justice Sotomayor expressed in her concurrence in *Jones*:

> It may be necessary to reconsider the premise that an individual has

---

110 *Id.*; Louise Matsakis, *The Supreme Court Just Greatly Strengthened Digital Privacy*, WIRED (June 22, 2018), https://www.wired.com/story/carpenter-v-united-states-supreme-court-digital-privacy/ (implying that "other sensitive digital information … [like] emails, smart-home appliances, and technology that is yet to be invented" are not yet safe).

111 *Carpenter*, 138 S. Ct. at 2217, 2221.

112 *Id.* at 2217, 2220.

113 *Id.* at 2218.

114 *Id.* at 2210.

115 *Id.* at 2228.

116 *Id.* at 2217, 2237 (Thomas, J., dissenting); *id.* at 2270 (Gorsuch, J., dissenting).

117 Smith v. Maryland, 442 U.S. 735, 742 (1979); *see* MARY MADDEN ET AL., PEW RESEARCH CTR., PUBLIC PERCEPTIONS OF PRIVACY AND SECURITY IN THE POST-SNOWDEN ERA 2, 3 (2014), https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf ("[Americans] are willing to make tradeoffs in certain circumstances when their sharing of information provides access to free services.").

> no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[118]

Technology adds a complex layer to evaluating privacy expectations.[119] The court in *Carpenter* had an opportunity to clarify exactly how the government can and should interact with technology. Yet, the narrow ruling in *Carpenter* made the rules of engagement even more confusing. *Carpenter* leaves many questions open and invites future arguments before the Supreme Court on the topics of technology and privacy. For example, unanswered questions include exactly how much digital data law enforcement may possess without a warrant and when a third party is required to disclose its business records.[120] While *Carpenter* did signal that the Fourth Amendment may protect other types of personal information held by third parties, such as records regarding location information, the case also raises questions about third-party files similar to CSLI.[121] As there was no constitutional limit discussed in *Carpenter* regarding CSLI, there is no legal limit meant to restrict location surveillance by law enforcement; the impacts of *Carpenter* reach far beyond CSLI, which fails to protect privacy interests while advancing the interest of government spying.[122]

## IV. VOLUNTARY CONVEYANCE AND ASSUMPTION OF RISK

The crucial question for the Supreme Court in deciding in favor of Carpenter focused on whether the automatic generation of CSLI is just a byproduct of having a cellphone; today, cellphones require no affirmative action.[123] In other words, as long as the phone is powered on and there is a cellphone tower near the phone's location, its location is being recorded and transmitted to the third-

---

118 United States v. Jones, 565 U.S. 400, 417–18 (2012) (Sotomayor, J., concurring) (citations omitted).

119 *Id.* at 427 (Alito, J., concurring).

120 *See Carpenter*, 138 S. Ct. at 2217 (holding the seizure of seven days of CSLI data constituted a Fourth Amendment search, but the court did not state how many fewer days would also constitute a search).

121 *Jones*, 565 U.S. at 417 (discussing the fact that advances in technology have led to people willingly disclosing to third parties more personal information than in the past).

122 *See Carpenter*, 138 S. Ct. at 2217 ("[W]e need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be. It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.").

123 *Id.* at 2220.

party cellphone carrier.[124]

Generally, voluntary conveyance is the premise that threatens the third-party doctrine in the technological era. For an action to be considered voluntary, it must have been intended, which presumes that the individual knew the relevant information would be conveyed.[125] Given how omnipresent and necessary technology and technological disclosures are, it is nearly impossible to deem these actions as voluntary.[126]

Prior cases involving privacy have referred to this voluntary participation as an "assumption of risk."[127] "When a party reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs, the Fourth Amendment does not prohibit governmental use of that information."[128] As a result of voluntary conveyance and the assumption of risk under the third-party doctrine, the government is permitted to investigate information disclosed to third-party businesses without a warrant.[129] However, merely allowing a device into one's life should not be enough to void one's privacy rights, which have been guaranteed to citizens since the time of this country's founding.

In *Carpenter*, the court declined to extend the third-party doctrine to CSLI as there was no voluntary exposure given that carrying a cellphone has become commonplace; in fact, the court even recognized this as "indispensable to participation in modern society."[130] The same will likely be true of other smart devices, including those found in smart homes.

An individual may initiate self-surveillance, for example, by purchasing an Amazon Echo or using a smartwatch; therefore, it could be argued that while using the basic functions of the device, the individual has affirmatively engaged

---

124 *The Problem with Mobile Phones*, SURVEILLANCE SELF-DEF., https://ssd.eff.org/en/module/problem-mobile-phones (last updated Oct. 30, 2018).

125 *Carpenter*, 138 S. Ct. at 2219–20; *see Voluntary*, BLACK'S LAW DICTIONARY (11th ed. 2019).

126 *See Carpenter*, 138 S. Ct. at 2210 (stating that a voluntary exposure of location information to a third-party does not hold up when it comes to CSLI because carrying a cell phone is indispensable to participation in modern society).

127 *See* Smith v. Maryland, 442 U.S. 735, 745 (1979); *see also* United States v. Miller, 425 U.S. 435, 443 (1976); Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

128 Denae Kassotis, *The Fourth Amendment and Technological Exceptionalism After Carpenter: A Case Study on Hash-Value Matching*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1243, 1275 (2019).

129 *Id.* at 1272.

130 *Carpenter*, 138 S. Ct. at 2220; *see* Trevor Timm, *The Government Just Admitted It Will Use Smart Home Devices for Spying*, GUARDIAN (Feb. 9, 2016), https://www.theguardian.com/commentisfree/2016/feb/09/internet-of-things-smart-devices-spying-surveillance-us-government/.

the device to relay a multitude of information.[131] However, the individual does not intend to share, nor could he or she ever imagine, the amount of information found on these devices, especially when this information is sent to other third parties to market products to consumers.[132] People connect to technology to establish and maintain relationships and function in society.[133] They voluntarily disclose detailed information about their private lives, such as information about religious views or sexual preferences, to social media platforms, including Facebook, Twitter, and LinkedIn, so they can participate in digital social life.[134] Many of these third-party service providers or social media platforms ask users to click "I Agree" after a long terms of service agreement or privacy disclosure agreement.[135] However, the average person does not have the time to read these lengthy documents, nor can they understand the complicated legalese that these agreements often contain.[136] Even if he or she can understand the complicated legalese, the individual typically fails to understand the ramifications of sharing the information or even the depths of information stored on him or her.[137]

## V. THIRD-PARTY DOCTRINE IMPACT ON TECHNOLOGIES

Self-cyber surveillance is the "intentional or consensual creation of mass information about oneself through electronic tracking or other means."[138] This self-cyber surveillance has changed the daily lives of many individuals and has altered the privacy of their information.[139] Assistive technologies present an issue in the accumulation of data retained by third-party businesses.[140] This data

---

131 Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. REV. 423, 441–42 (2018).

132 *See, e.g.*, *id.* at 429.

133 *See, e.g.*, Janna Anderson & Lee Rainie, *The Future of Social Relations*, PEW RES. CTR. (July 2, 2010), https://www.pewresearch.org/internet/2010/07/02/the-future-of-social-relations-2/.

134 *See generally* Joshua L. Simmons, *Buying You: The Government's Use of Fourth-Parties to Launder Data About "The People"*, 2009 COLUM. BUS. L. REV. 950, 990–91 (describing how companies can "provide lists of people who take Prozac for depression, believe in the Bible, gamble online, or buy sex toys").

135 *See* Kevin Litman-Navarro, *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster*, N.Y. TIMES, https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html (last visited Apr. 26, 2020).

136 *See, e.g.*, *id.*

137 *See, e.g.*, *id.* (describing how policies can be impenetrable for consumers as data collection measures become more sophisticated).

138 Steven I. Friedland, *Drinking from the Fire Hose: How Massive Self-Surveillance from the Internet of Things Is Changing the Face of Privacy*, 119 W. VA. L. REV. 891, 892 (2017).

139 *Id.*

140 The issue raised is only when the data resides in the cloud or in the hands of a third-party service provider. Data housed in the device is protected under *Riley*. Riley v.

creation and collection is described loosely as the Internet of Things ("IoT").[141] IoT is defined as the "aggregation of systems of networks connected to each other by the Internet or other radio-type device," which "creates consensual mass self-surveillance."[142] Because this includes any device with the ability to connect to the internet, a host of devices are included that seamlessly share information to "improve consumer, commercial, health, and other needs."[143] The records aggregated from these devices could consist of either metadata or content, or a mixture of both.[144] Examples of these devices include medicine dispensers that remind individuals to take their medicine,[145] thermostats that allow individuals to adjust their settings from a smartphone,[146] or even a trashcan that "scans the barcodes of discarded products, automatically adds them to a smartphone's shopping list, and sends a text when the trashcan is full."[147] IoT also includes in-home technologies, such as the Amazon Echo, and biometric data found on Apple Watches and FitBit devices.[148] The information shared with these devices can also be shared with other devices and applications.[149] Many of these devices operate by using the same passive data collection that smartphones do; in addition, the signals from the devices make them communication devices.[150] Thus, these devices are similar to cellphones and the reasoning behind CSLI protection in *Carpenter* should be extended to them.[151]

The aggregation of smart technology data also allows the government to work with corporations to create detailed reports on unsuspecting individuals who

---

California, 573 U.S. 373, 397 (2014).

141 Friedland, *supra* note 138, at 892; *see also The Internet of Things (IoT)*, SAS, https://www.sas.com/en_us/insights/big-data/internet-of-things.html (last visited Apr. 26, 2020).

142 Friedland, *supra* note 138, at 892–93.

143 Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 812 (2016).

144 *See generally id.* at 873 (discussing the distinction between metadata and content data).

145 Paul Kominers, *Interoperability Case Study, Internet of Things (IoT)*, BERKMAN CTR. FOR INTERNET & SOC'Y (Apr. 16, 2012), https://cyber.law.harvard.edu/node/97248.

146 *How Home/Away Assist Uses Your Phone's Location*, GOOGLE NEST HELP, https://support.google.com/googlenest/answer/9262475?hl=en (last visited Apr. 26, 2020).

147 Ryan G. Bishop, Note, *The Walls Have Ears, and Eyes, and Noses: Home Smart Devices and the Fourth Amendment*, 61 ARIZ. L. REV. 667, 668 (2019).

148 John A. Rothchild, *Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online (or Anywhere Else)*, 66 CLEV. ST. L. REV. 559, 573 (2018).

149 Yannis Bakos et al., *Shared Information Goods*, 42 J.L. & ECON. 117, 118 (1999).

150 Ferguson, *supra* note 143, at 818.

151 Christopher Mims, *All Ears: Always-On Listening Devices Could Soon Be Everywhere*, WALL ST. J. (July 12, 2018), https://www.wsj.com/articles/all-ears-always-on-listening-devices-could-soon-be-everywhere-1531411250.

may have committed crimes.[152] Since *Carpenter*'s narrow decision regarding CSLI, the third-party doctrine remains relatively undisturbed.[153] However, more information will continue to be shared with third-party service providers, especially with the advent of new technology. This allows for the disjunction between constitutional protections and technology surveillance and allows the gap between the two to become progressively more pronounced. In fact, the fear of government surveillance is not speculative; the government has requested data in the past, notably, to solve crimes, but it is not difficult to imagine this data being used in nefarious ways.

### A. Smart Home Devices

Smart home devices "connect the devices and appliances in your home so that they can communicate with each other and with you."[154] These devices are a natural progression of IoT. Accordingly, a smart home is defined by appliances or devices that are capable of connecting with one another through phone applications and the internet.[155]

The Amazon Echo is a smart home device that can respond to voice queries about the weather, turn down the lights or the temperature, and even order the groceries.[156] Alexa, Amazon's voice-activated digital assistant, powers Echo devices.[157] For the Echo to respond to the owner's request, it listens for the device activation word, "Alexa."[158] Meanwhile, the Echo "records your voice and transfers it to a processor for analysis"; the recordings are then streamed and stored remotely in the cloud where they can be reviewed at a later date.[159] The

---

152 *See* Timm, *supra* note 130.

153 Michael Gentithes, *The End of Miller's Time: How Sensitivity Can Categorize Third-Party Data After* Carpenter, 53 GA. L. REV. 1039, 1058 (2019).

154 Adrienne McClain, *Is the Government Using Your Refrigerator to Spy on You*, 19 W. MICH. COOLEY J. PRAC. & CLINICAL L. 327, 330 (2018); Molly Edwards & Nathan Chandler, *How Smart Homes Work*, HOWSTUFFWORKS, http://home.howstuffworks.com/smart-home1.htm (last visited Apr. 26, 2020).

155 Andrew Guthrie Ferguson, *The Smart Fourth Amendment*, 102 CORNELL L. REV. 547, 585 (2017).

156 Brief for Technology Companies as Amici Curiae Supporting Neither Party at 9, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402); *Alexa User Guide: Learn What Alexa Can Do*, AMAZON, https://www.amazon.com/b?node=17934671011 (last visited Apr. 26, 2020); Anne Pfeifle, *Alexa, What Should We Do About Privacy? Protecting Privacy for Users of Voice-Activated Devices*, 93 WASH. L. REV. 421, 440 (2018).

157 Pfeifle, *supra* note 156, at 421; *Alexa User Guide: Learn What Alexa Can Do*, *supra* note 156.

158 Pfeifle, *supra* note 156, at 421–22; *Alexa User Guide: Learn What Alexa Can Do*, *supra* note 156.

159 Eliott C. McLaughlin, *Suspect OKs Amazon to Hand over Echo Recordings in Murder Case*, CNN BUS. (Apr. 26, 2017), https://www.cnn.com/2017/03/07/tech/amazon-echo-alexa-bentonville-arkansas-murder-case/index.html; *Alexa User Guide: Learn What*

preferences expressed by an individual to his or her smart home device are used to create a comprehensive profile based on that specific consumer's activities, including his daily activities (through the calendar applications), or his health profile (through health monitoring applications);[160] this profile is then shared by third parties.

A specific example occurred in a widely publicized 2015 case, in which it was alleged that an Amazon Echo recorded audio of a man, James Bates, murdering his wife in his home.[161] Although Mr. Bates consented to the release of records held by Amazon, this story represents a cautionary tale regarding the information the Amazon Echo retains and is later available, information that the government can seize under the third-party doctrine.[162] These records contain some of our innermost thoughts, including details about our familial, professional, religious, and political ties.

On the one hand, because Echo users voluntarily convey this information to third parties, there are no Fourth Amendment protections implicated.[163] In contrast, Fourth Amendment jurisprudence has rendered the home supreme.[164] Justice Scalia indicated that at the core of the Fourth Amendment was the individual's "right to retreat into his own home" and to "be free from unreasonable governmental intrusion."[165] Furthermore, *Riley* concerns are implicated due to the capabilities of these smart home devices.[166] The home has been considered a sacred place since the time of the Framers and throughout Fourth Amendment history.[167] However, IoT has grown, mostly unregulated, and it is threatening the sanctity of the home.[168] Without a Fourth Amendment

---

*Alexa Can Do*, *supra* note 156.

160 *Alexa User Guide: Learn What Alexa Can Do*, *supra* note 156.

161 McLaughlin, *supra* note 159.

162 Arielle M. Rediger, *Always-Listening Technologies: Who Is Listening and What Can Be Done About It*, 29 LOY. CONSUMER L. REV. 229, 247 (2017).

163 Laura K. Donohue, *The Fourth Amendment in a Digital World*, 71 N.Y.U. ANN. SURV. AM. L. 553, 640 (2016).

164 *See* Donohue, *supra* note 41, at 1192; *see also* United States v. Karo, 468 U.S. 705, 714 (1984) ("At the risk of belaboring the obvious, private residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable.").

165 Florida v. Jardines, 569 U.S. 1, 13 (2013) (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)); *see also* Kyllo v. United States, 533 U.S. 27, 37 (2001) ("In the home . . . all details are intimate details.").

166 Adam Lamparello & Charles E. MacLeon, Riley v. California*: Privacy Still Matters, but How Much and in What Contexts*, 27 REGENT U. L. REV. 25, 36 (2014).

167 Stephanie M. Stern, *The Inviolate Home: Housing Exceptionalism in the Fourth Amendment*, 95 CORNELL L. REV. 905, 936 (2010).

168 *See generally Study Reveals Desire for MORE Regulation in IoT World*, BUSINESSWIRE (Feb. 12, 2018, 8:00 AM),

exception, if the police were to physically enter your home and seize your IoT device, later downloading the data, you would have a trespass to your property and effects, and therefore a violation of your privacy.[169] This concept becomes hazy when discussing an interception of your data on the device. This is because, as the Echo is always listening, the device serves as a covert listening device, informally, "a bug" or wiretap.[170] Although a user can delete the records that Alexa creates (although it is unclear how many records are deleted from the cache of information), it is strongly discouraged because the loss of records impairs the performance of the device.[171] Compelling individuals to sacrifice their privacy rights to their information stored by third parties for the sake of convenience is neither reasonable nor acceptable.

When an individual acquires a new device, he or she is most likely not rushing home to read the privacy policy.[172] Rather, he or she rushes home to install the new piece of technology and to start using it. This hastiness almost always results in the user relinquishing personal data in exchange for the use of the new device. For example, in 2015, Samsung was in the news for a privacy policy related to the use of its Smart TVs.[173] The company had initially cautioned customers that, through the use of voice recognition, data would be transmitted to third parties.[174] It did not take long for consumers and news outlets to begin reporting on the issue, comparing the Samsung Smart TVs to the telescreens featured in George Orwell's *1984*.[175] Following the backlash, Samsung changed the Smart TV privacy policy to state explicitly how the Voice Recognition technology worked. The new policy states:

> If you enable Voice Recognition, you can interact with your Smart

---

https://www.businesswire.com/news/home/20180212005111/en/Study-Reveals-Desire-Regulation-IoT-World (explaining that IoT workers view IoT as underregulated and in need of more government oversight and control).

169 *See* Silverman v. United States, 365 U.S. 505, 511–12 (1961) (emphasizing the higher degree of protection afforded to the home in Fourth Amendment jurisprudence).

170 Jeb Su, *Why Amazon Alexa Is Always Listening to Your Conversations: Analysis*, FORBES (May 16, 2019), https://www.forbes.com/sites/jeanbaptiste/2019/05/16/why-amazon-alexa-is-always-listening-to-your-conversations-analysis/#74fcdfb2378e.

171 Jing Cao & Dina Bass, *Why Google, Microsoft, and Amazon Love the Sound of Your Voice*, BLOOMBERG TECH. (Dec. 13, 2016), https://www.bloomberg.com/news/articles/2016-12-13/why-google-microsoft-and-amazon-love-the-sound-of-your-voice.

172 Meyer v. Uber Techs., Inc., 868 F.3d 66, 79 (2d Cir. 2017) (holding that a person can be held to the terms of a contract online without express acceptance).

173 *See, e.g.*, Andrew Griffin, *Samsung Smart TV Policy Allows Company to Listen in on Users*, INDEP. (Feb. 9, 2015), http://www.independent.co.uk/life-style/gadgets-and-tech/news/samsungs-new-smart-tv-policy-allows-company-to-listen-in-on-users-10033012.html.

174 Natasha Lomas, *Samsung Edits Orwellian Clause Out of TV Privacy Policy*, TECH. CRUNCH (Feb. 10, 2015), http://techcrunch.com/2015/02/10/smarttv-privacy/#.puzvmzo:yfMB.

175 *Id.*

> TV using your voice. To provide the Voice Recognition feature, your voice commands will be transmitted (along with information about your device, including device identifiers) to us and we will convert your voice commands into text to provide the Voice Recognition features. In addition, Samsung may collect voice commands and associated texts so that we can evaluate and improve the features. Samsung will collect your voice commands when you make a specific request to the Smart TV by clicking the activation button either on the remote control or on your screen or by speaking a wake word … and speaking into the microphone on the remote control or Smart TV.[176]

Samsung also clarified that individuals could opt-out of voice recognition if they had privacy concerns, but the capabilities would be impacted.[177]

B. Biometric Technology

FitBit devices, computing watches designed to track physical activity, raise additional concerns. Typically, the Fitbit monitors blood pressure, gives a sleep assessment, and counts steps, all of which is intended to help consumers gauge their personal health better.[178] This device also logs location information and uploads this information to a computer or mobile device if it is within range of a wireless internet source.[179]

This biometric data involves private information that, without the device, the individual most likely would not have; this information is extraordinarily intimate. However, this information can be "accessed, aggregated (even anonymized), and sorted by health companies or insurers to predict health trends and create more efficiencies in their businesses," which could pique the interest of other third parties and the government.[180] Yet, anonymity may not be enough to ensure privacy is protected.[181] In fact, according to one researcher, "[t]he way we move . . . is so unique that four points [of location information] are enough to identify 95% of people."[182]

---

176 *Samsung Privacy Policy for the U.S.*, SAMSUNG, https://account.samsung.com/membership/terms/privacypolicy (last visited Apr. 26, 2020).

177 *Id.*

178 Twomey, *supra* note 10, at 419.

179 *Why is the Fitbit App Prompting Me to Turn on Location Services?*, FITBIT, https://help.fitbit.com/articles/en_US/Help_article/2134 (last visited Apr. 26, 2020).

180 Friedland, *supra* note 138, at 897.

181 Bryan Lufkin, *The Reasons You Can't Be Anonymous Anymore*, BBC (May 29, 2017), https://www.bbc.com/future/article/20170529-the-reasons-you-can-never-be-anonymous-again.

182 Jason Palmer, *Mobile Location Data 'Present Anonymity Risk,'* BBC (Mar. 25, 2013), http://www.bbc.co.uk/news/science-environment-21923360.

The technology behind Fitbit devices is advanced enough that Fitbits can track physical exertion consistent with violent acts[183] or monitor the elevated blood pressure of someone under the influence of drugs.[184]

This newfound way of continued attachment to the digital world begs one major question: Would the information gathered, likely voluntarily, through various sources be considered a business record, thereby requiring third-party services to turn over the information on their customers?

### C. Internet Tracking

It is unclear whether *Carpenter* applies to all forms of location data, specifically geotags that are embedded in digital photographs and describe the time, date, and GPS coordinates of where a photograph was taken, as well as where the individual logged in to a social-media site if the photograph was posted.[185] Geotags are similar to CSLI because they are often automatically collected without affirmative action by the user.[186] However, they are slightly different because posting a picture on a public social media site is an affirmative action in which the user acknowledges that an indiscriminate group of people could see the post.[187] This is what happened to millionaire John McAfee, founder of McAfee Security Software Company.[188] McAfee was wanted by law enforcement in connection with a crime, and, although he threw out some taunts, authorities could not catch him, until a journalist took a photograph with McAfee and uploaded it online.[189] This photograph had been routinely geotagged, leading a computer hacker to MacAfee's exact location in a Guatemalan village.[190] While this case was a win for the police, this case should resonate with the average person. It was not difficult for the computer hacker to collect this information, even after MacAfee believed he had taken steps to conceal his

---

183 Christine Hauser, *Police Use Fitbit Data to Charge 90-Year-Old Man in Stepdaughter's Killing*, N.Y. TIMES (Oct. 3, 2018), https://www.nytimes.com/2018/10/03/us/fitbit-murder-arrest.html.

184 Ferguson, *supra* note 155, at 561.

185 GERALD FRIEDLAND & ROBIN SOMMER, INT'L COMPUT. SCI. INST., CYBERCASING THE JOINT: ON THE PRIVACY IMPLICATIONS OF GEO-TAGGING 1 (2010), https://www.usenix.org/legacy/events/hotsec10/tech/full_papers/Friedland.pdf.

186 *How to Challenge Cell-Site Location Information*, EFF, https://www.eff.org/criminaldefender/cell-site-location/how-challenge (last visited Apr. 27, 2020).

187 Ferguson, *supra* note 155, at 623–24.

188 Craig Timberg, *Hacker Locates John McAfee Through Smartphone Tracks*, WASH. POST (Dec. 4, 2012), https://www.washingtonpost.com/business/economy/hacker-locates-john-mcafee-through-smartphone-tracks/2012/12/04/55a498d8-3e4a-11e2-bca3-aadc9b7e29c5_story.html.

189 *Id.*

190 *Id.*

location.[191] Hackers with nefarious intentions could have uncovered this geotagged location, and, in the case MacAfee, who had not been accused of anything, the police could have then reviewed it for evidence.[192]

The government also has access to many of our routine activities. As Eleventh Circuit Judge Beverly Martin expressed:

> Nearly every website collects information about what we do when we visit. . . . [T]he Fourth Amendment allows the government to know from YouTube.com what we watch, or Facebook.com what we post or whom we "friend," or Amazon.com what we buy, or Wikipedia.com what we research, or Match.com whom we date—all without a warrant. In fact, the government could ask "cloud"-based file-sharing services like Dropbox or Apple's iCloud for all the files we relinquish to their servers. I am convinced that most internet users would be shocked by this.[193]

Individuals leave a digital footprint anytime they interact with devices that connect to the internet.[194] Paul Ohm, a professor at Georgetown Law Center and a privacy advocate, testified to Congress with respect to the trove of data collected by sources:

> The list of websites an individual visits, available to a [broadband internet access service] provider even when https encryption is used, reveals so much more than a member of a prior generation would have revealed in a composite list of every book she had checked out, every newspaper and magazine she had subscribed to, every theater she had visited, every television channel she had clicked to, and every bulletin, leaflet, and handout she had read. No power in the technological history of our nation has been able until now to watch us read individual articles, calculate how long we linger on a given page, and reconstruct the entire intellectual history of what we read and watch on a minute-by-minute, individual-by-individual basis.[195]

Web browsing records give the government access to an unprecedented amount of information, and a staggering amount is left unprotected.[196] For instance, individuals share information about themselves simply by surfing the

---

191 *Id.*

192 *See generally id.*

193 United States v. Davis, 785 F.3d 498, 536 (11th Cir. 2015) (en banc) (Martin, J., dissenting).

194 *See* Ferguson, *supra* note 155, at 585 (discussing a situation where an internet enabled thermostat was used to reveal confidential information about a homeowner).

195 Paul Ohm, Professor, Georgetown Univ. Law Ctr., Statement at FCC Overreach: Examining the Proposed Privacy Rules: Hearing Before the House Subcommittee on Communications and Technology (June 14, 2016).

196 *Davis*, 785 F.3d at 536 (en banc) (Martin, J., dissenting).

web because of the tracking methods websites use to store information.[197] One way websites track people is through cookies, which are small pieces of code sent back to the company that detail "whether you are a returning user, the sites you visited before, and after visiting their web site, the items you view on a web site, and sometimes even the information you enter into the computer while on the web site."[198]

D. Storage in the Cloud

Today, much of one's private data is held in the "cloud," which is defined as a "combination of structured, semistructured, and unstructured data collected by organizations that can be mined for information and used in … advanced analytics applications."[199] Essentially, the user "rents space" on a trusted server.[200] One may do this either because one's computer cannot store enough on its hard drive, for additional protection should a file be wiped off his or her computer, or both.[201] Many users find cloud storage extremely convenient, largely because the cloud can be accessed remotely.[202] Nevertheless, cloud storage is problematic because it requires users to give their data to a third-party service provider who then stores this vast quantity of information.[203]

Apple's iCloud Privacy Policy relating to cloud storage and law enforcement provides:

> You acknowledge and agree that Apple may, without liability to you, access, use, preserve and/or disclose your Account information and Content to law enforcement authorities, government officials, and/or a third party, as Apple believes is reasonably necessary or appropriate, if legally required to do so or if Apple has a good faith belief that such access, use, disclosure, or preservation is reasonably necessary to: (a) comply with legal process or request; (b) enforce this Agreement, including investigation of any potential violation thereof; (c) detect, prevent or otherwise address security, fraud or technical issues; or (d) protect the rights, property or safety of Apple, its users, a third party, or the public as required or permitted by

---

197 Derek S. Witte, *Bleeding Data in a Pool of Sharks: The Anathema of Privacy in a World of Digital Sharing and Electronic Discovery*, 64 S.C. L. REV. 717, 731–34 (2013).

198 *Id.* at 731.

199 Margaret Rouse, *Big Data*, TECH. TARGET, https://searchdatamanagement.techtarget.com/definition/big-data (last visited Apr. 27, 2020).

200 Erik C. Shallman, Comment, *Up in the Air: Clarifying Cloud Storage Protections*, 19 INTELL. PROP. L. BULL. 49, 54 (2014).

201 *Id.* at 50.

202 *Id.*

203 *See id.* at 50–51.

law.[204]

This privacy policy affords very little protection to consumers' data once the data is transferred to the Apple iCloud.

## VI. THE FUTURE OF THE CLOUD

The SCA, which is part of the ECPA, was an act created to regulate electronic communications.[205] However, it addresses the technology of the 1960s, thereby rendering it nearly ineffective to support privacy intrusions by the government on third-party servers that store and process the data that emanates from our modern devices.[206]

At the time of the SCA's enactment, "digital information still resided in large data centers" and "the data stored in data centers were not readily transportable."[207] Because people, and companies, store data everywhere, the question becomes: how should the SCA be interpreted in the digital age? According to the SCA, a warrant is not required if the data has been stored for more than 180 days.[208] This stipulation made sense during this time, as online storage of data in the cloud was extremely costly, and the IoT had not begun to aggregate data as it does now.[209] Privacy expectations should not diminish simply because 180 days have elapsed, just as privacy expectations do not diminish solely because time has passed.

This outdated language leads to another problem. The SCA defines electronic storage "both as 'any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof' and 'any storage of such communication by an electronic communication service for purposes of backup protection of such communication.' "[210] Privacy protections hinge on these crucial distinctions, but this second definition will cause problems with the popularity of the cloud, as the language of the statute excludes much of

---

204 *Welcome to iCloud*, APPLE, https://www.apple.com/legal/internet-services/icloud/en/terms.html (last updated Sept. 19, 2019).

205 Witte, *supra* note 197, at 748–49.

206 *See* Mark Wilson, Comment, *Castle in the Cloud: Modernizing Constitutional Protections for Cloud-Stored Data on Mobile Devices*, 43 GOLDEN GATE U. L. REV. 261, 263 (2013); Witte, *supra* note 197, at 749–50.

207 Wilson, *supra* note 206, at 263.

208 18 U.S.C. § 2703(a) (2012).

209 *See* Kalev Leetaru, *The High Costs of Hosting Science's Big Data: The Commercial Cloud to the Rescue?*, FORBES (Jan. 3, 2016), https://www.forbes.com/sites/kalevleetaru/2016/01/03/the-high-costs-of-hosting-sciences-big-data-the-commercial-cloud-to-the-rescue/#12344d4f28c0.

210 18 U.S.C. § 2510(17) (2012).

the data currently stored in the cloud.[211] It also does not account for how quickly and easily information can be accessed by a third party, which traditionally might have been stored on a computer's hard drive or in a file cabinet.[212] The immense amount of information stored in a cloud should be afforded greater protection than is currently provided. For example, much of the information stored through the third-party service Dropbox, a well-known cloud service provider, should be covered under the SCA.[213]

Essentially, the files in these servers are "papers" in modern electronic communications, making cloud storage entitled to an extension of Fourth Amendment protection if one acknowledges the modern-day technological equivalence of physical storage. In fact, "the cloud is merely an illusion," as information is stored on a physical server rather than a far-off intangible place, as the name would suggest.[214] The significant difference is that physical limitations found in traditional Fourth Amendment cases involving a physical intrusion are no longer commonplace in the digital age.[215] Still, in relation to the third-party doctrine, it remains unclear if cloud data can be considered business records.[216]

## VII. DISCUSSION OF CURRENT PRIVACY THEORIES

It is imperative that the Supreme Court establish a new precedent governing government access to third-party records. These theories will only be described insofar as they relate to technology.

### A. Reasonable Expectation of Privacy Test

Four decades have passed since Justice Harlan opined his reasonable expectation of privacy test in his *Katz* concurrence, and the meaning of the phrase is still unclear.[217] However, this test is still the cornerstone of many privacy rights cases.[218]

---

211 *See* Shallman, *supra* note 200, at 67.

212 *See id.* at 50.

213 *Id.* at 50–51 (explaining that Dropbox is a remote file-storage application that automatically syncs digital files to its servers upon the user's action).

214 Wei Chen Lin, *Where Are Your Papers?: The Fourth Amendment, the Stored Communications Act, the Third-Party Doctrine, the Cloud, and Encryption*, 65 DEPAUL L. REV. 1093, 1107 (2016).

215 *See id.* at 1095.

216 *See* Shallman, *supra* note 200, at 60.

217 *Expectation of Privacy*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/expectation_of_privacy (last visited Apr. 27, 2020).

218 *See* Peter Winn, Katz *and the Origins of the "Reasonable Expectation of Privacy" Test*, 40 MCGEORGE L. REV. 1, 1 (2009).

The reasonable expectation of privacy test is subjective and outdated. This test assumes that judges can effectively assess what a "reasonable" person would expect; however, there are two issues that arise from this test.[219] First, by assuming a judge can discern what a reasonable person might feel about a specific type of technology, this also assumes that the judge is up to date on all of the technologies people use on a daily basis.[220] In addition, it does not leave room for reasonable individuals to have differing opinions on what they see as, in this case, a reasonable intrusion of privacy.[221] Put simply, in a society that normalizes comprehensive surveillance, how "reasonable" is the average people, and who is the society? Does the average person's opinion come from the majority of people through a poll or survey? If so, this binds the minority thinkers to the preferences of the majority, thus ignoring the goal of the Bill of Rights of limiting the will of the majority.[222] The second issue is related to the outdated context of the test. It requires judges to consider new technology and then create policy based on how they perceive Americans might understand the latest technology and how the technology in question works.[223]

As it is currently understood, the expectation of privacy test is often the dominant theory cited when questioning Fourth Amendment protections.[224]

### B. Property/Trespass Theory

Physical intrusions, regardless of how major or minor the interference, can generate a Fourth Amendment violation under the trespass theory.[225] "The property-based approach emphasizes the historical reverence of property rights in the colonial era leading up to the American Revolution."[226] This approach was frequently used up until the 1960s when the *Katz* balancing test replaced it; the approach required individuals to prove that the government had physically trespassed onto their property before Fourth Amendment relief could be considered.[227]

---

219 *See id.* at 7.
220 *See id.* at 10.
221 *See id.* at 13.
222 SOLOVE, *supra* note 43, at 117.
223 Margaret Hu, *Cybersurveillance Intrusions and an Evolving* Katz *Privacy Test*, 55 AM. CRIM. L. REV. 127, 141 (2018) (discussing Justice Alito's explanation of a "tradeoff" individuals accept in diminished privacy for the increase of "convenience or security" of new technology).
224 *Id.* at 129.
225 *See* United States v. Jones, 565 U.S. 400, 404 (2012) (holding that placement of the GPS device without any other intrusion was a search).
226 Bishop, *supra* note 147, at 673.
227 Brady, *supra* note 27, at 949; *see also* Katz v. United States, 389 U.S. 347, 352–53

In 2012, *Jones* dusted off the old trespass doctrine when the court decided that a GPS attachment to a car used to monitor the vehicle's movements was a physical trespass.[228] In writing for the majority, Justice Scalia stressed the physical aspect of the search, reasoning that the government had intruded on the Defendant's privacy when it "inserted [an] information-gathering device."[229] However, the majority did not disturb the long-held privacy formulation defined in *Katz*, signaling an era in which Fourth Amendment protections were subjective and based on the type of trespass that occurred.[230] Justice Scalia most likely chose the property approach over the reasonable expectation of privacy test established in *Katz* because it was more straight-forward.[231]

C. Mosaic Theory

Privacy activist Orin Kerr explains the "Mosaic Theory" as an "aggregated set of data acquisitions," noting that a set of non-searches can amount to a search because the collection of the data and following analysis creates a revealing mosaic of a person's private life.[232] It is the aggregation of these movements, regardless of whether the movements occurred in public, that is worthy of protection.[233] A mosaic search might bring together locations and timeframes that illustrate a comprehensive picture of a suspect's life.[234] The problem with the Mosaic Theory, like with the current reasonable expectation of privacy theory, is the subjective nature of a violation. The quality of the mosaic will be different for each person, especially when considering the different kinds of surveillance tools that are available, which raise their own reasonableness concerns.[235] Courts will then be forced to construct a framework for deciding how much, or what kind of information can be gathered before a "search" has occurred.[236]

---

(1967) (rejecting the notion that physical penetration into a protected area is required to show a Fourth Amendment search).

228 *Jones*, 565 U.S. at 404–05, 410.

229 *Id.* at 410.

230 *See id.* at 411.

231 *See generally id.* at 407–08 (explaining that *Katz* preserved the right that an unconstitutional physical intrusion of an area may be a Fourth Amendment violation, and did not narrow the scope of the amendment).

232 Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 326, 333 (2012).

233 *Id.* at 326.

234 *Id.* at 313.

235 *Id.* at 333, 336.

236 *Id.* at 329.

D. Positive Law Theory

If a court decides to apply the positive law model, it considers whether there is a law (or statute, rule, or code), other than the Fourth Amendment, that restricts the government's invasion.[237] Positive law questions whether a search or seizure occurs by determining whether a private party could lawfully conduct the action the government engaged in.[238] Accordingly, instead of the court being concerned about a "reasonable search," it would ask, whether in completing the search, if the government official violated "general applicable law or avail[ed] themselves of a governmental exemption from it."[239]

Positive law may be problematic when new technologies arise because the cornerstone of this theory is reliance on existing law. The rate at which technology changes and adapts makes it nearly impossible for legislators to keep up with regulating emerging technologies, and even if they try, a backlog may result due to ever-changing technology.[240] It is also possible that some kinds of technology are so obscure that any sort of law regulating their use would be ill-advised.[241] Another roadblock preventing this theory from becoming a guiding precedent is the existence of technology that only the government has access to.[242] It may be possible for lawmakers to tweak the laws to allow private parties access to the technology to avoid Fourth Amendment scrutiny, fully knowing the private parties will never be able to access the devices.[243]

E. Equilibrium-Adjustment Theory

Equilibrium-Adjustment Theory is defined by privacy scholar Orin Kerr as the idea that the courts adjust "legal rules to restore the preexisting balance of

---

237 Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 516 (2007).

238 Richard M. Re, *The Positive Law Floor*, 129 HARV. L. REV. F. 313, 314 (2016).

239 William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1825–26 (2016).

240 *See* Re, *supra* note 238, at 327.

241 *See* Kyllo v. United States, 533 U.S. 27, 29 (2001) (holding the government used a device to complete a search that is not available to the general public, the search is unreasonable and requires a warrant). Although you may now buy the device used in question in *Kyllo*, it is not hard to convey this same holding to other devices not yet available to the public.

242 *See* Katie Barlow, *Thermal Imaging Gets More Common but the Courts Haven't Caught Up*, NPR (Feb. 27, 2014), https://www.npr.org/sections/alltechconsidered/2014/02/25/282523377/thermal-imaging-gets-more-common-but-the-courts-havent-caught-up; *see also Future Technology in Government*, INST. FOR GOV'T (May 21, 2019), https://www.instituteforgovernment.org.uk/explainers/future-technology-government.

243 Re, *supra* note 238, at 326.

police power."[244] Under this theory, if a case arose, the judge would adjust the level of protection for new technology to maintain this balance of power.[245] Kerr argues that the courts should decide this protection to restore a time which he calls "Year Zero."[246] Year Zero is a fictional time that is used as a basis to see how the "introduction of new tools poses a constant challenge to any legal system that seeks to regulate police investigations."[247]

This theory considers the dynamic nature of technology and social change,[248] and realizes that new tools and attitudes threaten the security and privacy balance between criminals and police because they allow both sides to "accomplish tasks they couldn't before" or undertake those tasks "more easily or cheaply than before."[249] The police should not possess so much power that they are able to infringe upon an individual's civil liberties, but they must also be powerful enough to enforce the law.[250] This theory is more of a method of maintaining the status quo of power rather than an effort to restore the Fourth Amendment to the Founder's original intent.

This theory only exacerbates the Fourth Amendment privacy judicial delay problem that the courts already face. Kerr argues this delay would be encouraged to ensure the courts do not make decisions about technology too quickly.[251] However, this delay would only complicate decisions due to the difficult to predict and progressive nature of IoT. This theory also requires judges to project their respective opinions on various technology-focused cases.

## VIII. THIRD-PARTY DOCTRINE AFTER *CARPENTER*

*Carpenter* could have been used to fundamentally change the third-party doctrine, but its narrow ruling raises questions and concerns about what kinds of digital data and how much data the government may access without a warrant; these concerns will likely continue to arise in future privacy cases.[252] However, *Carpenter* does provide a roadmap for future decisions as it disfavored the government's ability to claim "a significant extension of [the third-party doctrine] to a distinct category of information."[253] The court acknowledged that in order to live in modern society, the use of smart technologies is

---

244 Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 482 (2011).
245 *Id.* at 501.
246 *Id.* at 483.
247 *Id.*
248 *Id.* at 485.
249 *Id.* at 486.
250 *Id.* at 526.
251 *Id.* at 539.
252 *See* Barlow, *supra* note 242.
253 Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

"indispensable."[254]

Online vendors analyze buying preferences to suggest future, related purchases.[255] There is an electronic trail of when emails are sent and to whom they are sent.[256] Search engines collect inquiries and store them in case a user needs to revisit an old search.[257] The news applications on phones filter stories and suggest new ones based on past interests.[258] Home security cameras can be monitored from cellphones; doors and windows to houses can be locked from a smartphone.[259]

Professor Daniel Solove, an expert in the privacy field, considered the third-party doctrine to be "one of the most serious threats to privacy in the digital age."[260] The abandonment of the third-party doctrine should be favored and replaced with an approach that is neutral, regardless of the type of technology, to eliminate uncertainty and confusion over whether society has a reasonable expectation of privacy in the presence of certain technologies. In theory, a new approach should also allow the market to create new technologies and help consumers fully understand the privacy implications of the devices they purchase to permit informed decisions about using them. A new theory should also preclude the need to prosecute the privacy concerns over every new application, device, or company that maintains records about us.

As Justice Gorsuch explained in his dissent in *Carpenter*, the third-party doctrine is woefully incapable of reconciling Fourth Amendment protections in the modern age, stating, "Even our most private documents—those that, in other eras, we would have locked safely in a desk drawer or destroyed—now reside on third-party servers."[261]

The third-party doctrine should not apply with respect to certain technologies because much of the information forfeited by individuals is completed on behalf of their devices.[262] To waive Fourth Amendment protections, the individual must

---

254 *Id.* at 2220 (citing Riley v. California, 573 U.S. 373, 385 (2014)).

255 Lisa Magloff, *Examples of Targeted Advertising*, CHRON, https://smallbusiness.chron.com/examples-targeted-advertising-10869.html (last visited Apr. 27, 2020).

256 *Understanding Email Message Flow, from Sending to Delivery*, SPARKPOST, https://www.sparkpost.com/resources/email-explained/email-message-flow-sending-delivery/ (last visited Apr. 27, 2020).

257 Magloff, *supra* note 255.

258 *The Apple News App*, APPLE SUPPORT, https://support.apple.com/en-us/HT202329 (last visited Apr. 29, 2020).

259 *Can I Control My Home Security from My Phone?*, SAFEWISE (Feb. 6, 2020), https://www.safewise.com/home-security-faq/home-security-phone/.

260 Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 753 (2005).

261 Carpenter v. United States, 138 S. Ct. 2206, 2262 (2018) (Gorsuch, J., dissenting).

262 *See* Solove, *supra* note 260, at 753 (explaining the lack of voluntariness of people and

voluntarily provide information to a third party.[263] However, many device users do not voluntarily relinquish information; rather, when the devices are powered on, information is sent on behalf of the individual to third parties.[264] No voluntary action triggers this collection, and warrantless government searches conducted under the authority of the third-party doctrine should be unconstitutional. Because this is similar to the reasoning in *Carpenter*, this data collection should be given the same protections as CSLI.[265]

It is estimated that by 2027, forty-one billion IoT devices will be in use, up from eight billion in 2019.[266] This rapid expansion highlights the importance of establishing protections for data held by third parties, rather than just protecting CSLI.

## IX. REVISITING THE FOURTH AMENDMENT IN THE DIGITAL AGE

An awareness of the text and history of the Fourth Amendment and an understanding of modern technology is required for deciding privacy cases in the digital age. The understanding of what areas are constitutionally protected has grown to reflect changes in society and technology, with even originalist, conservative judges willing to expand protections to cover modern technologies.[267] In his dissenting opinion in *Carpenter*, Judge Gorsuch explained the importance of preserving the privacy that was intended since the adoption of the Fourth Amendment, stating that the Fourth Amendment must protect "specific rights known at the founding" and also their "modern analogues."[268]

The modern definitions of "papers" and "effects" are very complex compared to what the Framers had at the time of the Fourth Amendment. However, through the jurisprudence of the Fourth Amendment, one can see that they essentially serve the same purpose; emails are modern letters,[269] and computers are like file

---

the extensive data companies have that can be easily given to the government).

263 Smith v. Maryland, 462 U.S. 735, 743–44 (1979) (explaining the voluntary component of the third-party doctrine that waives Fourth Amendment protection).

264 *See* Josephine Wolf, *Losing Our Fourth Amendment*, N.Y. TIMES (Apr. 28, 2019), https://www.nytimes.com/2019/04/28/opinion/fourth-amendment-privacy.html.

265 *See Carpenter*, 138 S. Ct. at 2217.

266 Peter Newman, *THE INTERNET OF THINGS 2020: Here's What Over 400 IoT Decision-Makers Say About the Future of Enterprise Connectivity and How IoT Companies Can Use It to Grow Revenue*, BUS. INSIDER (Mar. 6, 2020), https://www.businessinsider.com/internet-of-things-report.

267 *See* Kyllo v. United States, 533 U.S. 27, 36 (2001) ("While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development.").

268 *Carpenter*, 138 S. Ct. at 2271 (Gorsuch, J., dissenting).

269 *See, e.g.*, United States v. Warshak, 631 F.3d 266, 284 (6th Cir. 2010).

cabinets.[270] The computers and software that store our digital footprints hold enormous amounts of data that could equal the massive amounts of data of the "papers" and "effects" the Founders envisioned.[271] Professor Davies, a well-known privacy scholar, has stated:

> In sum, although the evidence on this point is less than definitive, the available linguistic and statutory evidence suggests that "persons, houses, papers, and effects" was understood to provide clear protection for houses, personal papers, the sorts of domestic and personal items associated with houses, and even commercial products or goods that might be stored in houses—while leaving commercial premises and interests otherwise subject to congressional discretion.[272]

The text of the Fourth Amendment expresses the "right to be secure" in one's person, house, papers, and effects; the Framers intended to preserve that liberty against undue infringement, specifically state intrusion, by government officers regardless of the inevitable shifting of cultural norms.[273] Old-fashioned deposit receipts have been replaced by a digital paper.[274] When cars pass through a toll booth, an electronic record is created that logs the location and time of the passing.[275] The modern equivalent of papers the Framers stored in their desks is digital computer files.[276] Due to the history and purpose of the Fourth Amendment, "papers" should be read as an expressive analog to the more conventional, physical papers. This reading allows people to retain their guaranteed constitutional rights while also recognizing the role of technology and how it has altered the world. It is also necessary for this framework to work along a continuum. Information that is freely shared with others, for example, revealing comments left on public social media pages, deserves little to no protection.[277] Data that the user takes a concerted effort to restrict access to, data

---

270 *See, e.g.*, United States v. Williams, 592 F.3d 511, 523 (4th Cir. 2010) ("At bottom, we conclude that the sheer amount of information contained on a computer does not distinguish the authorized search of the computer from an analogous search of a file cabinet containing a large number of documents.").

271 Louise Matsakis, *The WIRED Guide to Your Personal Data (and Who Is Using It)*, WIRED (Feb. 15, 2019), https://www.wired.com/story/wired-guide-personal-data-collection/; Brady, *supra* note 27, at 981–83 (explaining the historical context and meaning of the words "papers" and "effects").

272 Davies, *supra* note 22, at 714.

273 U.S. CONST. amend. IV; Davies, *supra* note 22, at 744–45.

274 Ferguson, *supra* note 155, at 598.

275 *Id.*

276 *Id.* at 598–99.

277 Smith v. Maryland, 442 U.S. 735,744–46 (1979) (explaining that a person has no reasonable expectation of privacy to the information shared with others, thus, Fourth Amendment protection does not apply). Most data collected by smart devices will not be in

that contains deeply revealing information, or data that would typically be covered under the Fourth Amendment should be protected. This is due to the large amount of information that is held by third parties that, if shared, would threaten to expose some of people's innermost thoughts and questions, even bordering on characteristics that one would only share with his or her private diary or journal.

Under the existing doctrine, a gap exists in how to classify an "effect." The term "effects" has long been understood to extend to personal property;[278] in fact, the court has referenced objects such as automobiles[279] and luggage[280] as "effects" throughout its history. Due to the digital age, many scholars have suggested a broader reading of "effects" to cover computers, telephones, and other storage devices.[281] There is no reason why "effects" cannot be updated to be consistent with Fourth Amendment principles, as it would include the smart data, as well as signals emanating from the device.

The IoT offers new surveillance possibilities that do not require physical intrusion, resulting in the possibility of increased government surveillance that can reveal daily routines.[282]

The Fourth Amendment was not intended to define privacy; rather, like the rest of the Constitution, it is meant to recognize the necessity of limiting the government's power and discretion.[283] Despite new breakouts of technology, it is crucial that the Fourth Amendment is reevaluated to provide for traditional privacy limits because with current interpretations, the Fourth Amendment is

---

"plain view." However, information readily shared online through a public forum, with no additional skills or information required to access this information, will be an exception to the Fourth Amendment's warrant requirement.

278 Brady, *supra* note 27, at 982–83.

279 *See* Cady v. Dombrowski, 413 U.S. 433, 439 (1973) ("Although vehicles are 'effects' within the meaning of the Fourth Amendment, 'for the purposes of the Fourth Amendment there is a constitutional difference between houses and cars.' " (quoting Chambers v. Maroney, 399 U.S. 42, 52 (1970))); *see also* United States v. Jones, 565 U.S. 400, 404 (2012).

280 United States v. Place, 462 U.S. 696, 705–06 (1983); *see also* Florida v. Jimeno, 500 U.S. 248, 253 (1991) ("Luggage, handbags, paper bags, and other containers are common repositories for one's papers and effects, and the protection of these items from state intrusion lies at the heart of the Fourth Amendment.").

281 *See* Donald A. Dripps, *"Dearest Property": Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure*, 103 J. CRIM. L. & CRIMINOLOGY 49, 51 (2013) ("Portable devices like cell phones and flash drives are 'effects' subject to search and seizure like briefcases and backpacks."); *see also* Richard Sobel et al., *The Fourth Amendment Beyond* Katz, Kyllo and Jones*: Reinstating Justifiable Reliance as a More Secure Constitutional Standard for Privacy*, 22 B.U. PUB. INT. L.J. 1, 8 (2013).

282 *See* Ferguson, *supra* note 143, at 810.

283 *See* U.S. CONST. amend. IV (securing the "persons, houses, papers, and effects" of American citizens against unlawful searches and seizures, and requiring specificity of warrants based upon probable cause).

ineffective against certain government intrusions.

A. Technology or Privacy: Do You Have to Choose Just One?

Often, many people explain away their privacy by stating they have "nothing to hide," and because they are not doing anything wrong, they need not worry about the government having access to their information.[284] These explanations are known, respectively, as Nothing to Hide and All-or-Nothing.

*1. Nothing to Hide*

When discussing data privacy and technology, many people respond by saying they have nothing to hide. Variations of this argument include:
1. If you have nothing to hide, you have nothing to fear.[285]
2. "Like I said, I have nothing to hide. The majority of the American people have nothing to hide. And those that have something to hide should be found out, and get what they have coming to them."[286]
3. "Do I care if the FBI monitors my phone calls? I have nothing to hide. Neither does 99.99 percent of the population. If the wiretapping stops one of these Sept. 11 incidents, thousands of lives are saved."[287]

The issue with this line of reasoning is that it assumes everything should be public knowledge because nothing can be used against you. One journalist in *Time* asserted: "The more I learned about data-mining, the less concerned I was. Sure, I was surprised that all these companies are actually keeping permanent files on me. But I don't think they will do anything with them that does me any harm"; he further stated he was not worried because no human being ever reads the files.[288] This line of thinking is dangerous for two reasons: first, it fails to consider that some information may be perceived by government officials to be a pattern of criminal behavior, thereby giving the government a valid reason to monitor for criminal activity; second, these individuals sacrifice the rights of others because they do not care what happens to them.[289] Furthermore, individuals *could* read the files if they chose to, and, if a person was ever

---

284 SOLOVE, *supra* note 43, at 21.
285 Daniel J. Solove, *'I've Got Nothing to Hide' and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745, 747 (2007).
286 *Id.* at 749.
287 *Id.*
288 Witte, *supra* note 197, at 738–39.
289 SOLOVE, *supra* note 43, at 18 (discussing the use of governmental data mining for finding patterns to determine who is behaving suspiciously enough to warrant further government surveillance).

implicated in a crime, the government *could* seize the files and easily read about the person's whereabouts going back decades.[290]

Overall, this mindset leads to negative results, as it assists in the slow erosion of privacy rights over time.[291] For example, say the government begins to record telephone conversations arbitrarily. The individuals who support the nothing to hide theory may shrug their shoulders and brush the records off as minimal or non-invasive because the telephone conversation recordings are not widespread and, according to them, may cause at least one crime to be solved. To them, the benefits outweigh the risks. Alternatively, say the government begins monitoring some people's credit card statements in hopes of finding suspicious purchases. The individuals have not been flagged for suspicious purchases; rather the decision on who to monitor is pure chance. They may claim the government does not want to cause harm, which may be true, but the release of records may cause inadvertent harm. The more people who have access to the records, the more of a chance they will be leaked or the wrong person will gain access to them.[292] At first blush, these two examples may sound gradual but after a while, the government will have collected information on every American. What if the government takes this information and infers criminal activity?

### *2. All or Nothing*

Privacy and national security need not be mutually exclusive; surrendering privacy does not necessarily make citizens more secure, but surrendering security does not necessarily equate to an erosion of Fourth Amendment rights.[293] It is possible to allow for government oversight with "a degree of limitation" because the Fourth Amendment works through judicial oversight.[294]

This framework does not account for the nuances of technology. What if one wants to use Amazon Alexa to help organize his or her day, but this individual does not want it to provide his or her daily activities to the government freely? Currently, there are no provisions in place that would allow a person to accomplish this, other than not purchasing an Alexa (or other technology), due to the implementation and analysis of the third-party doctrine.[295]

---

290 Witte, *supra* note 197, at 739.

291 SOLOVE, *supra* note 43, at 12.

292 *See* Solove, *supra* note 285, at 768–69.

293 *See generally* SOLOVE, *supra* note 43, at 2 ("The privacy-security debate profoundly influences how these government activities are regulated . . . [these] arguments, however, are based on mistaken views about what it means to protect privacy and the costs and benefits of doing so.").

294 *See id.* at 4.

295 *See generally* THOMPSON II, *supra* note 7, at 7 (noting that the courts have long recognized a sweeping third-party doctrine where information willingly turned over to a third party is not subject to the same level of protection as other personal items).

This all or nothing mindset encompasses the third-party doctrine as it relates to technology not considered in *Carpenter*. Concerning CSLI and privacy cases that came before it, the All or Nothing Framework is better classified as Mostly All or Nothing.

## X. ALTERNATIVE SOLUTIONS

The Supreme Court is likely to address privacy jurisprudence, and new technologies, using the same piecemeal, incremental approach that has plagued old-fashioned common law.[296] The court has been reluctant to decide more than what stands before it, probably because judges do not feel they are able to fully understand contemporary technology or society's increasing desire to incorporate technology into daily routines.[297] Because this is the same judicial process that has brought us through *Carpenter*, it is imperative that society encourage private businesses or the legislature to step in and acknowledge privacy rights. To incentivize companies to safeguard consumers' privacy, it must first be "valued by consumers as a commodity in its own right, much like organic foods have become a valued food type."[298]

Companies should be responsible for safely collecting and transferring data, whether through the use of encryption on behalf of the company or partnerships with the government to encourage transparency.[299] The technology giants, such as Apple and Microsoft, should also stand up against governmental intrusion on behalf of their customers.[300] Consumers rely on them to protect their interests because the government can and will request consumers' data from them.[301]

### A. Encryption

Encryption is "the process of encoding information such that a key is required to decode it."[302] Encryption helps keep information secret from anyone who is not intended to have access to it through the use of a decryption key.[303]

---

296 *See id.* at 25–26.

297 *See id.* at 26.

298 Friedland, *supra* note 138, at 912.

299 *See Security Breach – How Businesses May Be Liable*, HG LEGAL RESOURCES, https://www.hg.org/legal-articles/security-breach-how-businesses-may-be-liable-44358 (last visited Apr. 29, 2020).

300 Riana Pfefferkorn, *Everything Radiates: Does the Fourth Amendment Regulate Side-Channel Cryptanalysis?*, 49 CONN. L. REV. 1393, 1405–06 (2017).

301 *Id.* at 1407–08.

302 David A. Couillard, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2217 (2009).

303 Pfefferkorn, *supra* note 300, at 1396; *What is Encryption? Types of Encryption*,

Encryption prevents the government, or anyone else, from gaining access to personal files and communications.[304] Currently, encryption provides a safe environment for internet and institutional commerce; so, it is not far off to assume that wider deployment of encryption to the public might be possible in the future.[305] This type of personal encryption would negatively impact law enforcement because encryption "makes it impossible, irrespective of warrants, for law enforcement to recover" the previously encrypted information.[306]

One privacy scholar contends that encryption to protect against a cyber-intrusion is analogous to physical locks, bolts, and alarms in a physical intrusion.[307] When encryption is afforded by companies, rather than individual consumers, the companies may provide discretionary access to the government as they have the keys to decrypt.[308] For example, WhatsApp offers end-to-end encryption for messages, voice calls, and videos.[309] Nevertheless, WhatsApp communication metadata is generally available to law enforcement, if required.[310]

In contrast, Apple has shown its unwillingness to support the government, despite its privacy policy.[311] Most notably, Apple would not create a backdoor for the encrypted cellphone of a deceased terrorist, Syed Farook in San Bernardino.[312] Apple was ordered by a federal magistrate judge to provide a backdoor to the government to allow federal investigators to determine if the terrorist was working alone.[313] Apple denied this request, asserting its commitment to ensuring the privacy of its millions of customers.[314] In the end, the government hacked the terrorist's phone without Apple's assistance.[315] However, this is not to say that Apple never hands over data to the government; in fact, Apple can and does disclose iCloud data to law enforcement.[316] The

---

CLOUDFLARE, https://www.cloudflare.com/learning/ssl/what-is-encryption/ (last visited Apr. 29, 2020).

304 Pfefferkorn, *supra* note 300, at 1396.

305 Lin, *supra* note 214, at 1095–96.

306 *Id.* at 1096.

307 Couillard, *supra* note 302, at 2225 (quoting WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT 721 (4th ed. 2004)).

308 *There Is No Middle Ground on Encryption*, ELECTRONIC FRONTIER FOUND. (May 2, 2018), https://www.eff.org/deeplinks/2018/05/there-no-middle-ground-encryption.

309 Pfefferkorn, *supra* note 300, at 1404.

310 *Id.* at 1411–12.

311 *See Welcome to iCloud*, *supra* note 204.

312 *Apple Still Doesn't Know How FBI Hacked San Bernardino Terrorist's iPhone Without Their Help*, FOX NEWS (Mar. 30, 2016), https://www.foxnews.com/tech/apple-still-doesnt-know-how-fbi-hacked-san-bernardino-terrorists-iphone-without-their-help.

313 *Id.*

314 *Id.*

315 *Id.*

316 Pfefferkorn, *supra* note 300, at 1412–13.

difference, theoretically, between these two cases is that in the terrorist attack, by providing the backdoor to the terrorist's phone, the government could conceivably hack all iPhone users with the touch of a button, whereas with the iCloud, the government must contact Apple in order to retrieve the information.[317] It may also be possible that the market will encourage individuals to better protect their privacy. As two technology advocates, Gershenfeld and Vasseur, concluded:

> By extending cryptography down to the level of individual devices, the owners of those devices would gain a new kind of control over their personal information. Rather than maintaining secrecy as an absolute good, it could be priced based on the value of sharing. Users could set up a firewall to keep private the Internet traffic coming from the things in their homes—or they could share that data with, for example, a utility that gave a discount for their operating their dishwasher only during off-peak hours or a health insurance provider that offered lower rates in return for their making healthier lifestyle choices.[318]

This suggestion allows consumers to choose whether they want to participate in the IoT, giving them the privacy many individuals desire while also allowing them to stay connected.

### B. Right to be Forgotten

Many legal scholars have suggested a "right to be forgotten" law, which draws its support and history from European countries.[319] This law is intended to secure private information for private individuals, as it allows individuals to have certain information deleted from search engines or places where internet records are stored.[320] It strives to balance data protection and the right of privacy with the public's interest in access to the information.[321] Critics contend that if a similar "right to be forgotten" law is adopted by Americans, there would be

---

317 *See generally* Thomas Brewster, *The Feds Can Now (Probably) Unlock Every iPhone Model in Existence*, FORBES (Feb. 26, 2018), https://www.forbes.com/sites/thomasbrewster/2018/02/26/government-can-access-any-apple-iphone-cellebrite/#3f4dcb37667a (discussing the U.S. government's ability to access data on iPhone models).

318 Neil Gershenfeld & J. P. Vasseur, *As Objects Go Online: The Promise (and Pitfalls) of the Internet of Things*, FOREIGN AFF., Mar.–Apr. 2014, at 60, 67.

319 John W. Dowdell, *An American Right to Be Forgotten*, 52 TULSA L. REV. 311, 314 (2017).

320 *Id.* at 321.

321 Eric Posner, *We All Have the Right to Be Forgotten*, SLATE (May 14, 2014, 4:37 PM), https://slate.com/news-and-politics/2014/05/the-european-right-to-be-forgotten-is-just-what-the-internet-needs.html.

profound impacts on the First Amendment Constitutional rights of freedom of speech and freedom of the press.[322] They claim it would be antithetical to one of the nation's founding principles: the free flow of information; they claim it amounts to censorship.[323] Secondly, critics argue that to allow private companies to remove certain information puts corporations in charge of enforcing privacy rights, thereby becoming the ones in charge of enforcing the balance between free speech and privacy.[324] On the other hand, supporters of a right to be forgotten law in the United States say it will allow individuals to better control their personal data.[325] They argue that much of the information online can be used to damage individuals and their respective futures.[326]

Currently, there are laws that cover many aspects of personal privacy in transactions, but they are not as encompassing as the right to be forgotten. Two examples include the Health Insurance Portability Accountability Act ("HIPAA") and the ECPA.[327] Both of these acts regulate the use of personal information.[328]

### C. Congressional Interception

An essential feature of society is the relationship between humans and the government; specifically, the checks and balances system enacted through the founding documents and the nature of the Republic. Individuals should be more vigilant about what information they disclose.[329] However, new developments in technology continue to maximize third-party disclosures.[330] Congress has the opportunity to craft legislation, with the Constitution in mind, that is amicable to law enforcement and the public, unlike the judiciary which can only rule on cases and laws that come before it.[331]

Consumers could benefit from federal privacy legislation as this would at

---

322 *See* Dowdell, *supra* note 319, at 334.

323 May Crockett, Comment, *The Internet (Never) Forgets*, 19 SMU SCI. & TECH. L. REV. 151, 174 (2016).

324 *See generally id.* at 178 (discussing the right to be forgotten and posing the question of companies like Google enforcing individual privacy rights).

325 *Id.* at 174.

326 *Id.*

327 *Id.* at 171.

328 *Id.*

329 *What Can You Do to Protect Your Data Online?*, FORBES (May 7, 2018), https://www.forbes.com/sites/quora/2018/05/07/what-can-you-do-to-protect-your-data-online/#1ba05dee68e2.

330 LEE RAINIE & JANNA ANDERSON, PEW RESEARCH CTR., THE FATE OF ONLINE TRUST IN THE NEXT DECADE 51 (2018), https://www.pewresearch.org/internet/2017/08/10/theme-3-trust-will-not-grow-but-technology-usage-will-continue-to-rise-as-a-new-normal-sets-in/.

331 SARAH HERMAN PECK, CONG. RESEARCH SERV., R44967, CONGRESS'S POWER OVER COURTS: JURISDICTION STRIPPING AND THE RULE OF *KLEIN* 1 (2018).

least present a baseline that all companies would follow.[332] As long as this baseline has consequences for those who do not comply, it would allow for nearly all companies to play by the same rules because the internet and other online devices cross state lines.[333] The legislation should be broad enough to account for rapidly changing technology, but narrow enough to ensure data security and privacy.[334] Furthermore, if companies wanted to take additional precautions to protect privacy, they should be welcome to do so under this new law.[335]

## XI. CONCLUSION

The digital transition from physical papers and the well-known concept of "effects" represents a dangerous time for citizens' civil liberties. The enumeration of the Fourth Amendment protections reflects the Founders' commitment to the development of thoughts, ideas, and beliefs. It is necessary that the Fourth Amendment is read to apply to all digital information, as a functional equivalent to the physical papers and effects that existed during the time of the Founding Fathers, if the United States is to preserve the right to privacy for future generations. The Founding Fathers could not have ever imagined the progression of technology, but their ideas and the foundation for the Fourth Amendment protecting certain things remains the same.

Supreme Court jurisprudence regarding privacy has been plentiful, but the court's decisions have focused on the devices rather than focusing on the types of information collected by devices in general. The cornerstone for many of these decisions has been the Fourth Amendment concept of reasonableness, but what is reasonable with respect to electronic data is neither clear nor consistent. As smart devices and internet tracking become even more prevalent, there is an urgent need to retire the third-party doctrine and reconsider the outdated nature of the SCA. *Carpenter* was a step in the right direction for CSLI, but it did not consider the vast array of technologies and the methods of data collection yet to emerge.

Americans *must* ensure the rights that were guaranteed by the Constitution at the time of founding are still applicable for digitization, regardless of the new

---

332 Jack Karston, *How Should the US Legislate Privacy?*, BROOKINGS (July 30, 2018), https://www.brookings.edu/blog/techtank/2018/07/30/how-should-the-us-legislate-data-privacy/.

333 *Id.*

334 Cameron F. Kerry, *Why Protecting Privacy Is a Losing Game Today—and How to Change the Game*, BROOKINGS (July 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/.

335 RAINIE & ANDERSON, *supra* note 330.

technologies that develop in the IoT. The Constitution may have been written a long time before cellphones and the internet were devised, but its beliefs of personal autonomy and privacy are unwavering.

Today, most of the information is stored on third-party servers; if this information can be obtained without a warrant, Fourth Amendment privacy protections are meaningless. If the third-party doctrine, as it stands, were to be applied to the IoT, the government would be given unlimited access to an individual's personal information as part of a comprehensive IoT profile.

In *Carpenter*, the court declined to extend the third-party doctrine to the data collected by cellphones, but this narrow interpretation only creates more questions than it answers. The smart home will soon be as much of a necessity to modern life as cellphones. The eroding roots of voluntary conveyance and assumption of risk of the third-party doctrine require a re-examination of the doctrine.

Consumers should be encouraged to care about their privacy and advocate to private businesses the importance of privacy. If lawmakers want to be involved, they should develop a comprehensive, timeless protocol to guide law enforcement in digital searches.